Remarks

In the application, claims 1 through 15 are pending. No claims currently stand allowed.

The Office Action dated October 14, 2003, has been carefully considered. The Office Action rejects claims 1 and 8 under 35 U.S.C. § 103(a) as obvious in light of Bruce Schneier, "Applied Cryptograph" and U.S. Patents 6,311,218 ("Jain") and 5,684,951 ("Goldman"). Claims 2 and 15 are rejected as obvious in light of Jain and U.S. Patent 6,336,186 ("Dyksterhouse"). Claims 3 through 7 and 9 through 14 are rejected as obvious in light of Jain, "Applied Cryptography," and Goldman.

The Office Action correctly points out that the registry 86, discussed in the paragraph beginning on page 13, line 4, of the specification, is not shown in Figure 1. The registry 86 is shown correctly in Figure 2, so the specification is amended to refer to Figure 2 instead of to Figure 1.

Two other paragraphs of the specification, the Abstract, and claims 3 and 12 are amended to correct minor informalities.

Claims 1 and 8 are amended to clarify the role of the network data.

The present application describes a user-authentication scheme that is "out-of-band," that is to say, that is outside of the protocols used to transmit "network" data. ("Network" data means data that are not transmitted solely as part of the user-authentication scheme.) The user authenticates himself via a public/private encryption key-based, challenge/response mechanism. However, because this authentication scheme is out-of-band, the existing data transmission protocol cannot make use of the authentication. Therefore, there needs to be some way to associate the authenticated user with the network data actually transmitted by the user. The present invention solves this by encrypting a portion of the user's transmitted network data into a "message digest" and by then making the encrypted message digest part of the authentication process. Only the authenticated user has the knowledge needed to correctly perform this encryption. The policy agent that performs the authentication compares the network data transmitted by the user with the message digest, which it can decrypt. If they match, then the policy agent knows that these network data must have been transmitted by the authenticated user.

The network data are thus *used* in the authentication scheme of the present invention, but they do not exist *solely* as part of the authentication scheme. The user transmits them primarily in order to perform some network task other than authentication (to query a database or to retrieve a web page, for example). Once the network data are associated with an authenticated user, the policy agent can decide whether to accept them for their non-authentication purpose (probably by passing them on to their intended recipient). Network data that cannot be associated with an authenticated user can be rejected (for example, see the specification, page 14, lines 15 through 24).

Claims 1 and 8 are amended to clarify this role of the network data, that is to say, to show that the network data are transmitted *both* for an authentication purpose *and* for a non-authentication purpose. The network data are not transmitted *solely* as part of the authentication scheme.

In a manner somewhat similar to the present invention, Jain describes a user-authentication scheme based on a public/private encryption key, challenge/response mechanism. However, Jain's authentication mechanism is entirely *in-band*, so that it does not need to address the problem of associating in-band network data with an out-of-band user-authentication. Neither does Goldman. Thus, while Jain and Goldman discuss the role of user data in the authentication process (of course), they do not discuss the use of that *same* data for some purpose beyond user authentication. Neither Jain nor Goldman, either separately or in combination, anticipate or render obvious the following elements of the independent claims (as currently amended):

> Claim 1:
>
> comparing the first and second message digest values to determine whether a match is found; and
>
> *deciding whether to accept the received network data*, the deciding based, at least in part, on a result of the comparing step.
>
> Claim 8:
>
> comparing the first and second message digest values to determine whether there is a match therebetween, and
>
> *deciding whether to accept the received network data*, the deciding based, at least in part, on a result of the comparing step.

(Emphasis added.) The portions of Jain and Goldman pointed to by the Office Action discuss the use of data *within* the authentication process. Their data are *not* used for a non-authentication purpose.

As the combination of the cited art neither anticipates nor renders obvious these independent claims, and as all other currently pending claims depend from these two claims, applicants request that the rejections be withdrawn and that all currently pending claims be allowed.

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

John Bretscher

John T. Bretscher, Reg. No. 52,651
One of the Attorneys for Applicants
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312)616-5600 (telephone)
(312)616-5700 (facsimile)

Date: January 28, 2003